#9

10/3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Patent Application of: )
Mark J. Buxton )
)
Serial No.: 09/505,211 ) Art Unit: 2134
Filed: February 16, 2000 )
) Examiner: Ellen C. Tran
For: Method and System for Providing )
Content-Specific Conditional )
Access to Digital Content )

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

## APPEAL BRIEF
## IN SUPPORT OF APPELLANT'S APPEAL
## TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicant (hereafter "Appellant") hereby submits this Brief in triplicate in support of his Appeal from a final decision by the Examiner in the above-captioned case. Appellant respectfully requests consideration of this Appeal by the Board of Patent Appeals and Interferences for allowance of the claims in the above-captioned patent application.

An oral hearing is not desired.

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231, ON: 15 APRIL 2004
Date of Deposit

INTEL CORPORATION
Name of Assignee

SIGNATURE 4/15/04
DATE

## I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

## II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

## III. STATUS OF THE CLAIMS

Claims 1-33 are pending in the above-referenced patent application. Claims 1-33 were rejected in the Final Office Action mailed on March 8, 2004. Claims 1-33 are the subject of this appeal.

## IV. STATUS OF AMENDMENTS

An amendment was filed on January 14, 2004, and was considered by the Examiner prior to issuing the Final Office Action.

A copy of all claims on appeal (claims 1-33) is attached hereto as Appendix A.

## V. SUMMARY OF THE INVENTION

Typical existing conditional access systems require objectionable content to be obfuscated at the source of the content (e.g., the broadcaster or content creator) or blocked at a viewer's site using circuitry in a receiver. With embodiments of the present invention, portions of digital content may be obfuscated at any level of a content distribution hierarchy. This allows each intermediate distributor to decide whether obfuscation will be performed and to describe how the obfuscation will be performed.

Embodiments of the present invention are a system and method for providing content level masking of digital content that is broadcast, multicast, or otherwise distributed to receivers in a communications system. Instead of controlling the content only at the location of the broadcaster or at the receiver, the present invention provides the capability to securely control access to the content, and manipulate the content itself via a masking operation, at any point in the digital content distribution hierarchy or transmission chain.

Embodiments of the present invention specify the use of a mask to change the content distributed to a receiver. The mask may be, for example, a distorted or opaque two dimensional (2D) region (for video content), or a replacement audio segment (for audio content), or a distorted or opaque three dimensional (3D) volume (for 3D content), carried separately from the original content in digital multimedia broadcast, multicast, or point-to-point distribution systems. The present invention also specifies the co-transmission to a receiver of encrypted, masked content, which may be used to "undo" a masking operation previously performed anywhere upstream in the distribution channel. The present invention provides for controlled, revocable access by an end-user to the content according to the policies of the content creator, owner or distributor. In one embodiment, this control mechanism may be used to protect selected audiences from being able to render objectionable content and to grant certain customers or distributors control over the level of masking or obfuscation performed on the content prior to rendering or further downstream transmission.

Figure 1 shows how the masks may be carried separately from the digital content in a transmission system. Depending on whether the *transmission channel* is *trusted* or *un-trusted* (in the computer security context), and depending on whether a *receiver* is *trusted* or *un-trusted* (again in the computer security context), different processing is performed on the digital content by distribution entities in the system. This processing is described in Figures 6 and 7, and the associated text in the Specification at page, line 12 to page 11, line 22, and recited in claims 1-5 and 12-16, and claims 6-11 and 17-22, respectively.

Generally, digital content may be transmitted in the present invention in three different formats. First, the content may be transmitted "in the clear", that is, in unedited and unmasked form as originally authored. Figure 2 shows content transmitted "in the clear", without any masking being applied to it. A variation on this format is shown in Figure 3, where the content is transmitted unobfuscated and a mask is sent along with the original content, thereby allowing any authorized element in a distribution hierarchy to apply the mask to the content to obfuscate selected portions of the content according to the specifications of the mask. Second, the content may be transmitted with a mask already applied to it to generate "*content after mask applied*" *(CAMA) data.* This term (CAMA data) is explicitly defined in the

Specification. This modified content may have had objectionable or sensitive data or information masked so that the objectionable or sensitive data or information cannot be perceived by the end-user. Figure 4 shows content after the mask has been applied as a selected portion of a content stream. Third, the content may be transmitted in "*content after mask applied" (CAMA)* format, but the transmission of data may also include the masked content after encryption has been performed (that is, the part of the content "cut out" by the mask). Figure 5 shows a portion of content after the mask has been applied along with the encrypted masked content in a transmission stream.

At each stage of the content authoring and distribution system of the present invention, system entities decide how to transmit the content. An entity may transmit the original content only, transmit the original content and associated mask for future application of the mask, apply the mask to the content and transmit the CAMA data only, or apply the mask to the content and transmit the encrypted masked content separately from the CAMA data, so that a downstream entity may reverse the masking operation if authorized to do so.

With the present invention, the audience (determined individually, via other members of an audience such as parents or corporate management, or via third parties such as governmental regulatory groups) can influence or control the selection or absence of masks by directly influencing the application of masks at each stage of the content distribution hierarchy. As shown in Figure 1, for some receivers, the resulting rendered content may be without obfuscation 30, but for other receivers, the rendered content may be with obfuscation 32, 34.

Figures 8-11 describe a content distribution system and processing performed by a content creator, content distributor, and receiver. This system is recited in claims 23-31. The content creator analyzes the content and identifies content regions to be masked for one or more versions of the content. The content distributor determines the security of the transmission channel and determines an associated distribution mode. Content distributor processing is recited in claims 32-33. The receiver determines how to process received content based on whether the channel is trusted and on what kind of data was received from a distributor.

## VI. ISSUES PRESENTED

A. Whether claims 1-3 and 12-14 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool, (US Pat. No. 6,373,948)(hereinafter Wool) in view of Aras et al. (US Pat. No. 5,872,588)(hereinafter Aras).

B. Whether claims 6-9 and 17-20 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool in view of Aras.

C. Whether claims 23-31 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool in view of Aras.

D. Whether claims 32-33 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool in view of Aras.

E. Whether claims 4, 10, 15, and 21 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool in view of Aras, and further in view of Ritchey (US Pat. No. 5,495,576).

F. Whether claims 5, 11, 16, and 22 are unpatentable under 35 U.S.C. 103(a) as being obvious over Wool in view of Aras, and further in view of Shoff et al. (US Pat. No. 6,240,555)(hereinafter Shoff).

## VII. GROUPING OF CLAIMS

For the purposes of this appeal:

Claims 1-3 and 12-14 stand or fall together as Group I.

Claims 6-9 and 17-20 stand or fall together as Group II.

Claims 23-31 stand or fall together as Group III.

Claims 32-33 stand or fall together as Group IV.

Claims 4, 10, 15, and 21 stand or fall together as Group V.

Claims 5, 11, 16, and 22 stand or fall together as Group VI.

## VIII. ARGUMENT

In rejecting claims under 35 U.S.C. § 103(a), it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1998). The examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hosp. Sys. Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). The determinations by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). If that burden is met, the burden then shifts to the applicant to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. See Id.; In re Hedges, 783 F.2d 1038, 1039, 228 USPQ 685, 686 (Fed. Cir. 1986); In re Piasecki, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984); and In re Rinehart, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

For the present application, the Examiner has not fulfilled her burden of presenting a prima facie case of obviousness. Therefore, the appealed claims are allowable.

### A. REJECTION OF CLAIMS 1-3 and 12-14 (GROUP I) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL AND ARAS IS IMPROPER. NEITHER WOOL NOR ARAS, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

Independent claim 1 recites the limitations of obtaining the digital content and a mask, determining if a receiver is *trusted*, sending the digital content to the receiver when the receiver is trusted (i.e., in the clear, no mask being applied to the data), and applying the mask to the digital content to generate *"content after mask applied"* data and sending the *content after mask applied data* to the receiver when the receiver is *not trusted.* As recited, the application of the mask to generate *content after mask applied data* (CAMA data) is required to be performed prior to sending the content (now modified) to the receiver. Implicitly, this means that application of the mask is done upstream from the receiver by a distribution entity in the content transmission hiearchy, not by the receiver. As recited, an untrusted receiver cannot receive digital content that is not masked.

Wool describes a system for providing restricted access to packages of TV programs, typically in a cable TV system. In Wool, cryptographic techniques are used to control access by a viewer to only selected subsets of TV programs or programming packages (i.e., to allow access only to those programs/channels registered for or paid for by the viewer). The Examiner seeks to apply Wool as teaching the claimed limitation "applying the mask to the digital content to generate content after mask applied data" (as noted on page 3, lines 7-9 of final Office action mailed March 8, 2004). However, Wool uses a mask as a filter only as a technique for determining which specific TV programs are part of certain programming packages (See col. 10, lines 13-25 of Wool) in order to allow the viewer's receiving device to determine the appropriate decryption key, and thus gain viewing access to the desired TV program. Wool's mask is applied by the receiver to the programming stream to determine if the receiver is authorized to display the entire TV program being received. Wool does not teach or suggest that masks can be applied to the content itself (i.e., the TV program) to modify portions of the content (as currently claimed and described in the Specification at page 7, lines 3-19), and further that this modification is done prior to sending the masked content to the receiver. That is, Wool does not teach or suggest that a mask can be applied to digital content (e.g., frames of a TV program) to obfuscate selected portions of that content so a viewer cannot perceive the selected portions of the content when the program is rendered for the viewer by a receiving device (e.g., a set top box or TV). *Wool's use of a mask is entirely different than the claimed invention.* Wool does not teach or suggest such obfuscation using masks as is currently claimed and as described in the Specification. Thus, the Examiner's reliance on this purported teaching of Wool is in error.

In response to this argument, the Examiner asserts in the final Office action that she relies instead on Aras at col. 10, lines 18-20 to teach this claim limitation (please see final Office action paragraph 25 on page 13). This assertion is false. The final Office action of March 8, 2004 clearly and explicitly states on page 3, lines 7-9 that Wool at col. 10, lines 11-12 is being relied on as purportedly teaching the limitation. Regardless, this claim limitation is also not taught or suggested in Aras.

Aras discloses an interactive TV program distribution system that allows a broadcaster to gather real-time information about the viewing behavior of subscribers. Information is collected by coding audio-visual materials (AVM) sent to viewer's receiving devices, and then by reporting the codes of the materials actually watched by the viewer to a collection center for processing. In col. 10, lines 9-30, Aras briefly refers to a parental control feature whereby objectionable language may be muted, yet no details on how this may be accomplished are provided. In Aras, this activity is clearly performed at the viewer's receiving device. In this regard, Aras teaches nothing more than what is well known in the parental control circuitry of many television sets today (that of blocking display of TV programs having a certain rating by the TV). In marked contrast, in the present invention, and as is currently claimed in claim 1, the masking of selected portions of the content to obfuscate such portions is performed ***prior*** *to* sending the "*content after mask applied*" data to the receiver, when the receiver is *not trusted*. <u>That is, the masking is applied by an entity other than the receiver, and done upstream in the content transmission hierarchy.</u> This is apparent from claim 1 since the application of the mask is done <u>before</u> the sending of the masked content to the receiver. Aras does not teach or suggest that an entity "upstream" in the content distribution system from the receiver applies the mask to the selected content as currently claimed (in the present invention, the masking can be done by any upstream entity in a hierarchical content distribution system). Claim 1 clearly recites steps taken by an entity other than the viewer's receiving device. Therefore, Aras does not teach or suggest the claimed limitation either. Since neither Wool nor Arras teach or suggest the claimed limitation of applying the mask to the digital content to generate content after mask applied data prior to sending the content after mask applied data to the receiver, the rejection of claim 1 on this basis is wrong and must be withdrawn.

Further, the meaning of the recited term "*content after mask applied*" data is clearly defined in the Specification. See page 6, lines 16-20 ("Second, the content may be transmitted with a mask already applied to it to generate "content after mask applied" (CAMA) data. This modified content may have had objectionable or sensitive data or information masked so that the objectionable or sensitive data or information cannot be perceived by the end-user.") This term is specifically recited in the claimed limitation. It is fundamental that an Applicant can be his or her own lexicographer. The CAMA data is selected content after it has been masked in such as way as to have certain portions obfuscated. This concept is clearly not taught or suggested by Wool, since masking in Wool merely refers to masking program identifiers in a topic hierarchy for identifying selected programs that have been purchased by the viewer as part of a cable TV marketing package. Similarly, Aras does not teach or suggest the concept of "content after mask applied" data being generated prior to sending to a receiver. Thus, neither Wool nor Aras teaches or suggests the claimed limitation.

Furthermore, the claimed limitation "sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is *not trusted*" is not taught or suggested in Wool or Aras, alone or in combination. Wool only sends data that is usable to a viewer's receiving device that is already *trusted* (i.e., is authenticated as being a device that is allowed to access the content due to the previous registration or paid subscription of the viewer). Wool does not modify the content (program) to obfuscate selected portions of the content to make those portions appear different to the viewer, when rendered, than the original content and then send that masked content to an untrusted receiver. Wool does not teach or suggest that the content is masked in this way (to generate "content after mask applied" data) so that when the content is rendered by the viewer's receiving device, objectionable content is obfuscated. Wool does not teach or suggest that masked content may be sent to a receiver that is *not trusted*, since Wool's receiver is assumed to be trusted before any usable content is sent.

In Aras, there is no determination of trust at all in a receiver. Yet claim 1 requires one action when the receiver is trusted and another action when the receiver is not trusted. The Examiner cites to col. 10, lines 21-24 of Aras in the final Office action at page 3 ("when home station determines that AVM are to be screened") as teaching the determination of trust. However, the cited text teaches nothing about a distribution entity determining whether a viewer's receiving device is trusted or not. Aras merely mentions that the receiver determines whether to block display of the TV program or not based on a program rating (which is typically included in the TV program itself). This has nothing to do with determining trust in the receiver itself by another entity, as is currently claimed.

Finally, one skilled in the art would not be motivated to combine the teachings and suggestions of the two cited references, because the combination would not result in the claimed invention. The combination does not teach or suggest masking of selected content and distribution of the masked content to downstream entities in a content distribution hierarchy as described in the present Specification and currently claimed. The combination does not teach or suggest sending original digital content to a receiver when the receiver is trusted, and sending masked content when the receiver is not trusted. In response, the Examiner argues in the final Office action at page 16, that motivation to combine the references exists because Aras at col. 1m line 27 teaches "Broadcast and/or Interactive television may be distributed over a variety of means, including but not limited to....In most cases, interactive television will co-exist with broadcast television." The Applicants fail to see how this argument presents a coherent foundation for a motivation to combine references. It is submitted that the Examiner has not presented a prima facie case of obviousness because the motivation to combine the references is lacking.

In sum, for at least the foregoing reasons, neither Wool nor Aras, either alone or in combination, teach or suggest claim 1 because several claim limitations are not met by the cited art, and there is no adequate motivation to combine the references because the combination would not result in claim 1. Therefore, claim 1 is allowable as presented.

Similarly, independent claim 12 is also allowable.

Accordingly, the claims dependent from claims 1 and 12 (claims 2-3 and 13-14) are also allowable.

### B. REJECTION OF CLAIMS 6-9 and 17-20 (GROUP II) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL AND ARAS IS IMPROPER. NEITHER WOOL NOR ARAS, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

Regarding the rejection of independent claims 6 and 17, many of the claimed limitations are not taught or suggested by the cited references.

1) As discussed above for claim 1, the cited references do not teach or suggest a mask being used to obfuscate selected portions of the content.

2) Neither of the references teach or suggest determining if the transmission channel for distributing the content is trusted. The Examiner cites Aras at col. 10, lines 21-24 as disclosing this limitation, but the cited text merely mentions determining whether to screen the content. This is not the same as determining trust in the cryptographic sense. The cited text does not teach or suggest the limitation.

In response to this point the Examiner argues on page 16 of the final Office action dated March 8, 2004 that this limitation is not recited in the rejected claims. This assertion is wrong. Claim 6 clearly recites the limitation ("determining if a channel for distributing the content is trusted"). See also claim 7 ("when the channel is trusted, performing the following"....).

3) As discussed above for claim 1, the cited references do not teach or suggest applying a mask to the content itself at a point in the content transmission hierarchy upstream from the receiver to generate masked content wherein part of the content is obfuscated ("content after mask applied" data). Claim 6 includes "applying the mask to the digital content to generate content after mask applied data and masked content" ... "sending the content after mask applied data and the encrypted masked content to a receiver". Claim 6 requires that application of the mask is performed when the channel is not trusted. The final Office action cites Aras, col. 10, lines 11-12 as teaching this limitation ("Program identifiers, p, are assigned to programs in the topic hierarchy 600 using the notion of prefix masks."). However, the cited text teaches nothing about the claimed limitation.

4) The limitation of encrypting the masked content is not taught or suggested. The cited text of Wool merely discloses that the TV program is transmitted as encrypted data to the receiver. In Wool's system, the mask is used to determine access to TV programs by the receiver. That is, <u>the receiver</u> applies the mask to the received data to determine if the receiver is eligible to display the data based on the viewer's subscription. If the viewer is eligible, then the receiver decrypts the encrypted program. In Wool, the *encrypted program* is not masked at all. In the present invention, a distribution entity upstream from the receiver <u>applies the mask to the content</u> (e.g., the TV progam) to produce "content after mask applied" data. This masked data is then encrypted and sent to the receiver to protect the masked data from unauthorized access. These concepts are very different from each other. Furthermore, Aras does not teach or suggest encrypted masked content either.

5) The limitation of reversing the masking is not taught or suggested. Wool merely teaches decrypting the encrypted program data and displaying it by the receiver. Wool does not teach or suggest that masked content that has been distributed (as discussed above and in the Specification) may be processed by the receiver to "reverse" the prior masking step performed by a distribution entity. That is, the receiver restores the original content (prior to the masking) when the receiver is trusted. This claimed limitation is very different than merely decrypted encrypted programs. In addition, Aras does not teach or suggest reversing the masking operation to reproduce original content when the receiver is trusted.

The final Office action at page 5 cites to Wool at col. 1, lines 41-43 as teaching the limitation of sending content after mask applied data and the encrypted masked content to a receiver, decrypting masked content, and reversing masking to reproduce original content for subsequent rendering when the receiver is trusted. However, a reading of the cited text ("provides the customer with a set-top terminal (STT) containing one or more decryption keys which may be utilized to decrypt programs that a customer is entitled to") shows that the cited text does not teach or suggest the claimed limitation of claim 6.

Since these limitations of claims 6 and 17 are not taught or suggested by the cited references, claims 6 and 17 are allowable as presented. All claims dependent therefrom (claims 7-9 and 18-20, respectively) are also allowable.

Furthermore, with respect to claims 7 and 18, this claim recites determining if a receiver is trusted when the transmission channel is trusted, and performing different processing depending on whether the receiver is trusted or not. Neither Wool nor Aras, alone or in combination, teach or suggest the limitations of claims 7 and 18, since neither reference teaches or suggests determining if a transmission channel is trusted.

## C. REJECTION OF CLAIMS 23-31 (GROUP III) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL AND ARAS IS IMPROPER. NEITHER WOOL NOR ARAS, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

With respect to independent claim 23, the combination of Wool and Aras does not teach or suggest the claimed invention. Claim 23 recites a content censor to identify regions of content to obfuscate, and a mask generator to accept the content and regions, and produce a mask to apply to the content to obfuscate the identified regions. Note blocks 206 and 212 of Figure 8 of the Specification for identification of the content censor and mask generator of the present invention. The final Office action cites Wool at col. 9, lines 53-67 ("utility of the present invention, care must be taken to ensure that the program identifier, p, assigned to programs of related content") and Aras at col. 10, lines 18-20 ("Thus, objectionable language may be silenced when the video portion is presented.") as teaching claim 23. The Applicant contents that the combination of Wool and Aras are wholly deficient in teaching or suggesting the claimed limitations. Where does Wool or Aras disclose a content censor to identify *regions of content* to obfuscate? Where does Wool or Aras describe producing a mask to apply to the content to obfuscate the identified regions? The Applicant contends these limitations are not found in Wool or Aras. The cited text certainly does not teach or suggest the claim.

The final Office action refers at page 17 to the "home station" of Aras and baldly asserts that this "home station" identifies regions to be obfuscated. Yet, a close reading of the cited text reveals that Aras does not teach or suggest anything about identifying regions to obfuscate and generating masks as described in the present Specification and currently claimed.

A region is defined in lines 1-6 of page 12 of the Specification. The meager reference in Aras to silencing audio while displaying video is not the same as the claimed content censor to identify regions of content to obfuscate. Furthermore, neither Wool nor Aras teach or suggest a mask generator to accept the content and regions (as determined by the content censor) and produce a mask to apply to the content to obfuscate the identified regions. As discussed at length above, Wool's mask is used to determine programming package subscriptions, not obfuscation of selected portions of content as currently claimed. The cited text of Aras does not teach or suggest that a mask can be applied to content to obfuscate identified regions as claimed. Since all of the claimed limitations are not taught or suggested, claim 23 is allowable as presented.

Because independent claim 23 is allowable, all claims depending on claim 23 (claims 24-31) are also allowable. Nevertheless, the Applicant wishes to comment on some of the deficiencies in the stated rejections of some of these claims.

As to claim 24, it recites the limitations of "wherein the mask generator links the content with the regions, generates a mask, applies the mask to the content to produce content after mask applied data and masked content, and encrypts the masked content." The cited text from Wool relied on by the Examiner to reject the claim teaches or suggests nothing about the claimed limitations ("if a customer is entitled to a particular program, the set-top terminal 300 will be able to derive the program key, Kp, from stored and received information", Wool at col. 5, lines 26-29). Wool does not use a mask generator to link content with regions (since Wool teaches nothing about regions of content to be masked), generate a mask to be applied to the content to obfuscate selected portions of the content, nor apply the mask to the content. Further, Wool does not teach or suggest encrypting masked content.

In response, the Examiner in the final Office action argues that the Applicant has attacked only one (i.e., Wool) of the two references being relied on by the Examiner. But Wool is the reference cited by the Examiner as purportedly teaching the claim limitation! The Applicant does not understand the confusing reliance on the case law of *In re Keller* and *In re Merck* when the Examiner has relied on only one of the references to teach the specific claimed limitation. It is submitted that the Examiner is improperly applying the principles of this case law to the present situation, and that the rejection of the claim must be withdrawn. At any rate, neither Wool nor Aras teach or suggest the limitations of claim 24. Therefore, claim 24 is allowable.

As to claim 26, neither Wool nor Aras sends content that has already been masked to the receiver. In Wool, the receiver does the masking of programming IDs to determine receiver eligibility for certain TV programs. In Aras, the "home station" (i.e., the receiver) may silence objectionable language. But neither Wool nor Aras teach or suggest transmission of masked content. Hence, claim 26 is allowable.

As to claim 27, Wool does not send content that has already been masked to the receiver. In Wool, the receiver does the masking of programming IDs to determine receiver eligibility. Wool does not teach or suggest transmission of masked content. Furthermore, Aras does not teach or suggest transmitting content after mask applied data and encrypted masked content to a receiver. Neither Wool nor Aras, alone or in combination, teach the limitations of claim 27. Claim 27 is allowable.

As to claim 29, neither Wool nor Aras teach or suggest that the masked content may be processed to reverse the masking and restore the obfuscated portions of the content to reproduce the original content. The cited text of Wool does not teach or suggest this limitation. Neither Wool nor Aras teaches anything about a de-masker.. Therefore, claim 29 is allowable.

As to claim 31, the claim requires that a content censor includes a region identification tool to identify a region of the digital content to obfuscate by applying the mask. The final Office action cites Aras as teaching "the screener mechanism may work in cooperation with an obscuration mechanism"... (Aras col. 10, lines 21-25). Aras mentions that something in the receiver may obscure some part of the AVM. Aras does not teach or suggest that a region ID tool used by a content creator identifies regions of content to obfuscate. Wool does not teach or suggest the limitation either. Neither Wool nor Aras, alone or in combination, teach or suggest claim 31. Therefore, claim 31 is allowable.

## D. REJECTION OF CLAIMS 32-33 (GROUP IV) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL AND ARAS IS IMPROPER. NEITHER WOOL NOR ARAS, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

With respect to independent claim 32, several limitations are not taught or suggested by the cited art. First, the cited art does not determine the security of the *transmission channel.* Wool teaches that the receiver may only display programs that the viewer is eligible to receive. But Wool does not determine the security of the transmission/distribution channel itself. Neither does Aras. This limitation is not taught or suggested by the combination of Wool and Aras. The final Office action contends that this limitation is taught by Aras at col. 22, line 60 through col. 23, line 9 ("collecting behavior information on channels"...). However, collecting behavior information is not the same as nor does it suggest determining the security of a transmission channel. Merely collecting behavior information does not teach or suggest the claimed limitation (which requires an assessment of channel security).

Second, the limitation of determining a mode of content distribution is not disclosed. The cited text of Aras does not match the claimed limitation. Third, as discussed at length above, the masking and obfuscation of content as described in the present Specification and currently claimed is not taught by the references. Fourth, claim 32 requires that the determination of trust of the transmission channel affects what processing is then done. When the channel is trusted, a first mode of operation is undertaken (as described in Figure 6); when the channel is not trusted, a second mode of operation is undertaken (as described in Figure 7). This concept is specifically recited in claim 32, but is not taught or suggest in the cited art. The cited text of Aras merely refers to identifying audi-visual materials. It does not teach or suggest two modes of operation depending on whether it is known that the transmission channel is trusted or not as currently claimed (and as described in the Specification at page 8, line 31 to page 9, line 14).

For at least the above reasons, claim 32 is allowable because a prima facie case of obviousness has not been presented.

Since claim 33 depends from allowable claim 32, it is also allowable.

## E. REJECTION OF CLAIMS 4, 10, 15, and 21 (GROUP V) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL, ARAS AND RITCHEY IS IMPROPER. NEITHER WOOL NOR ARAS NOR RITCHEY, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

Claims 4, 10, 15, and 21 recite the limitation that the digital content comprises three dimensional volume data and the mask comprises a replacement three dimensional region for a selected portion of the digital content. The Examiner cites Ritchey as teaching the claimed limitation. Ritchey appears to have no relevance to the claimed invention other than that it generally discloses 3D computer graphics. Ritchey does not teach or suggest that the content distributed by a content distribution entity is 3D volume data and that a mask may be applied to the 3D volume data to obfuscate a selected portion of the 3D volume by replacing the selected portion with other data. Since Ritchey does not teach or suggest the claimed limitation, the combination of Wool, Aras, and Ritchey do not teach or suggest the claims. Since the Examiner relies on Ritchey as teaching the 3D volume data and replacement 3D region limitation of claims 4, 10, 15, and 21, the Applicants do not understand the repeated citation to the case law of *In re Keller* and *In re Merck* in the final Office action. It is submitted that the Examiner is improprely relying on this case law in sustaining the rejection. Since Ritchey does not teach or suggest the claimed limitation, the combination of Wool, Aras, and Ritchey does not teach or suggest these claims because the Examiner has relied on Ritchey to supply the missing teaching that is deficient in Wool and Aras for these claims. Furthermore, these claims are dependent on allowable independent claims. Thus, claims 4, 10, 15 and 21 are allowable as presented.

## F. REJECTION OF CLAIMS 5, 11, 16, and 22 (GROUP VI) UNDER 35 U.S.C. § 103(a) UNDER THE COMBINATION OF WOOL, ARAS AND RITCHEY IS IMPROPER. NEITHER WOOL NOR ARAS NOR RITCHEY, ALONE OR IN COMBINATION, TEACH OR SUGGEST ALL OF THE CLAIM LIMITATIONS. THEREFORE, A PRIMA FACIE CASE OF OBVIOUSNESS HAS NOT BEEN MADE.

Claims 5, 11, 16, and 22 require that application of the mask results in replacement of part of the content with a replacement creative component. That is, the objectionable content portion is obfuscated by replacing it with another, unobjectionable content portion. However, in Shoff, the system includes additional supplemental content broadcast to a receiver that is displayed concurrently with the main TV program on the display. In essence, the supplemental content of Shoff is shown in one location of the display while the regular TV program is shown in the remainder of the screen (e.g., similar to a picture in picture (PIP) feature). This is very different than replacing a selected portion of the content of a frame of video with other content by applying a mask. Shoff does not teach or suggest using a mask to replace content portions. Shoff displays additional data, but does not provide replacement of a selected portion of content. Since Shoff does not teach or suggest the claimed limitation, the combination of Wool, Aras, and Shoff does not teach or suggest these claims because the Examiner has relied on Shoff to supply the missing teaching that is deficient in Wool and Aras for these claims. Furthermore, these claims are dependent on allowable independent claims. Therefore, claims 5, 11, 16, and 22 are allowable.

## IX. CONCLUSION

Appellant respectfully submits that all the pending claims in this patent application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted in triplicate, along with the funds to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(c). Please charge any shortages and credit any overcharges to Deposit Account No. 02-2666.

Respectfully submitted,

Date: 4/15/04

Steven P. Skabrat

Steven P. Skabrat
Intel Corporation
Attorney for Appellants
Registration Number: 36,279

c/o Blakely, Sokoloff, Taylor & Zafman
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8598

X. APPENDIX A: CLAIMS ON APPEAL

1. (Original) A method of content level filtering and distribution of digital content in a content distribution system comprising:

obtaining the digital content and a mask for obfuscating a selected portion of the digital content;

determining if a receiver of the digital content is trusted;

sending the digital content to the receiver for subsequent rendering when the receiver is trusted; and

applying the mask to the digital content to generate content after mask applied data and sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

2. (Original) The method of claim 1, wherein the digital content comprises video data and the mask comprises a replacement two dimensional region for a selected portion of one or more frames of video data.

3. (Original) The method of claim 1, wherein the digital content comprises audio data and the mask comprises a replacement audio clip for a selected portion of the digital content.

4. (Original) The method of claim 1, wherein the digital content comprises three dimensional volume data and the mask comprises a replacement three dimensional region for a selected portion of the digital content.

5. (Original) The method of claim 1, wherein application of the mask results in replacement of a selected portion of the digital content with a replacement creative component.

6. (Original) A method of content level filtering and distribution of digital content in a content distribution system comprising:

obtaining the digital content and a mask for obfuscating a selected portion of the digital content;

determining if a channel for distributing the content is trusted;

when the channel is not trusted, performing the following:

applying the mask to the digital content to generate content after mask applied data and masked content;

encrypting the masked content;

determining if a receiver of the digital content is trusted;

sending the content after mask applied data and the encrypted masked content to a receiver, decrypting the masked content, and reversing masking to reproduce original content for subsequent rendering when the receiver is trusted; and

sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

7. (Original) The method of claim 6, further comprising:
when the channel is trusted, performing the following:

determining if a receiver of the digital content is trusted;

sending the digital content to the receiver for subsequent rendering when the receiver is trusted; and

applying the mask to the digital content to generate content after mask applied data and sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

8. (Original) The method of claim 6, wherein the digital content comprises video data and the mask comprises a replacement two dimensional region for a selected portion of one or more frames of video data.

9. (Original) The method of claim 6, wherein the digital content comprises audio data and the mask comprises a replacement audio clip for a selected portion of the digital content.

10. (Original) The method of claim 6, wherein the digital content comprises three dimensional volume data and the mask comprises a replacement three dimensional region for a selected portion of the digital content.

11. (Original) The method of claim 6, wherein application of the mask results in replacement of a selected portion of the digital content with a replacement creative component.

12. (Original) An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide content level filtering and distribution of digital content in a content distribution system by:

obtaining the digital content and a mask for obfuscating a selected portion of the digital content;

determining if a receiver of the digital content is trusted;

sending the digital content to the receiver for subsequent rendering when the receiver is trusted; and

applying the mask to the digital content to generate content after mask applied data and sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

13. (Original) The article of claim 12, wherein the digital content comprises video data and the mask comprises a replacement two dimensional region for a selected portion of one or more frames of video data.

14. (Original) The article of claim 12, wherein the digital content comprises audio data and the mask comprises a replacement audio clip for a selected portion of the digital content.

15. (Original) The article of claim 12, wherein the digital content comprises three dimensional volume data and the mask comprises a replacement three dimensional region for a selected portion of the digital content.

16. (Original) The article of claim 12, wherein application of the mask results in replacement of a selected portion of the digital content with a replacement creative component.

17. (Original) An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide content level filtering and distribution of digital content in a content distribution system by:

obtaining the digital content and a mask for obfuscating a selected portion of the digital content;

determining if a channel for distributing the content is trusted;

when the channel is not trusted, performing the following:

applying the mask to the digital content to generate content after mask applied data and masked content;

encrypting the masked content;

determining if a receiver of the digital content is trusted;

sending the content after mask applied data and the encrypted masked content to a receiver, decrypting the masked content, and reversing masking to reproduce original content for subsequent rendering when the receiver is trusted; and

sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

18. (Original) The article of claim 17, further comprising instructions for:

when the channel is trusted, performing the following:

determining if a receiver of the digital content is trusted;

sending the digital content to the receiver for subsequent rendering when the receiver is trusted; and

applying the mask to the digital content to generate content after mask applied data and sending the content after mask applied data to the receiver for subsequent rendering of the content after mask applied data when the receiver is not trusted.

19. (Original) The article of claim 17, wherein the digital content comprises video data and the mask comprises a replacement two dimensional region for a selected portion of one or more frames of video data.

20. (Original) The article of claim 17, wherein the digital content comprises audio data and the mask comprises a replacement audio clip for a selected portion of the digital content.

21. (Original) The article of claim 17, wherein the digital content comprises three dimensional volume data and the mask comprises a replacement three dimensional region for a selected portion of the digital content.

22. (Original) The article of claim 17, wherein application of the mask results in replacement of a selected portion of the digital content with a replacement creative component.

23. (Original) A system providing content level filtering and distribution of digital content comprising:

a content censor to identify regions of content to obfuscate; and

a mask generator to accept the content and regions and produce a mask to apply to the content to obfuscate the identified regions.

24. (Original) The system of claim 23, wherein the mask generator links the content with the regions, generates a mask, applies the mask to the content to produce content after mask applied data and masked content, and encrypts the masked content.

25. (Original) The system of claim 23, further comprising a distributor to transmit the content and the mask to a receiver.

26. (Original) The system of claim 23, further comprising a distributor to transmit content after mask applied data to a receiver.

27. (Original) The system of claim 23, further comprising a distributor to transmit content after mask applied data and encrypted masked content to a receiver.

28. (Original) The system of claim 25, wherein the receiver comprises a masker to apply the mask to the content to produce content after mask applied data for rendering by the receiver.

29. (Original) The system of claim 27, wherein the receiver comprises a decryptor to decrypt the encrypted masked content and a de-masker to reverse masking of the content after mask applied data to reproduce original content for rendering by the receiver.

30. (Original) The system of claim 23, further comprising a content creator to create the digital content.

31. (Original) The system of claim 23, wherein the content censor comprises a region identification tool to identify a region of the digital content to obfuscate.

32. (Original) A method of distributing digital content in a hierarchical content distribution system comprising:

determining security of a transmission channel;

determining a mode of content distribution;

when the mode is a first mode performing:

obtaining the digital content and a mask to apply to the digital content to obfuscate selected portions of the digital content when the transmission channel is trusted; and

obtaining content after mask applied data when the transmission channel is not trusted;

when the mode is not a first mode, obtaining content after mask applied data and encrypted masked content; and

sending obtained data to other entities in the hierarchical content distribution system.

33. (Original) The method of claim 32, further comprising sending the obtained data to at least one receiver.